

Systems of Systems and Security: A Defense Perspective

Kristen Baldwin, kristen.baldwin@incose.org; Judith Dahmann, judith.dahmann.ctr@osd.mil; Jonathan Goodnight, jonathan.goodnight@incose.org

.....
*DoD is working to
 integrate security into
 the systems engineering
 tradespace for designing
 and acquiring military
 systems.*

Today's dynamic defense environment is characterized by an array of changing threats, with innovative, rapidly adaptive strategies to collect information, disable systems, and disrupt the adversaries' ability to mount and sustain an effective defense. This threat environment has led to heightened awareness of system vulnerabilities and has made security a key concern for operations and now for defense acquisition. Both in addressing operational security issues in the current inventory of legacy systems and in looking forward, the US Department of Defense (DoD) is placing increasing emphasis on addressing security considerations as part of system acquisition and engineering.

Concurrently, most defense systems today operate as part of one or more *systems of systems*, often in a networked environment. To implement the war-fighting strategies of today and tomorrow, systems are networked and designed to share information and services in order to provide a flexible and coordinated set of war-fighting capabilities. Under these circumstances, systems operate as part of an ensemble of systems supporting broader capability objectives. This move to a system-of-systems (SoS) environment poses new challenges to systems engineering in general and to specific DoD efforts to engineer secure military capability.

This article examines the current United States defense approach to security and the challenges posed by systems of systems. We intentionally do not address challenges that are not unique to systems of systems. Although the situation we are describing is specific to the defense domain, we believe that the issues also apply beyond the defense community to other areas including integrated transportation systems, financial systems, and other critical infrastructure.

The Department of Defense's Current Approach to System Security

Historical approaches to system security focused on preventing unauthorized access to information. Personnel security ensures that clearances and a "need to know" are in place before people obtain access. Network security ensures that identities are authen-

ticated prior to information exchange. Security has focused on keeping critical technology and information from "getting out." However, as DoD systems have come to depend on commercial technology and components that are increasingly sourced through complex global supply chains, a new security emphasis is emerging: keeping malicious threats or compromised system elements or components from "getting in." Mitigating the opportunity for critical capabilities to be compromised through the supply chain or system design is a relatively new focus for the defense department, and it requires systems engineering expertise that has not been involved in acquisition security.

To address this challenge, DoD is working to integrate security into the systems engineering tradespace for designing and acquiring military systems. A July 2009 *INSIGHT* article outlined a vision for what this integration would achieve (Baldwin 2009). Acquisition programs would identify mission-critical technology, components, and information. Make/buy decisions for critical components would be made in a risk-informed manner, and systems engineers would allocate security requirements to system components. The department's recent activities to achieve this vision include the following:

- Publishing a research roadmap for establishing system-security engineering as a fundamental discipline of systems engineering (Bayuk et al. 2010)
- Tailoring applicable methods and processes, such as criticality analysis, from nearby disciplines (e.g., safety, reliability) to a security perspective
- Developing Systems Engineering Technical Review (SETR) criteria for system security

The DoD is beginning to implement the products of these efforts into individual systems on a program-by-program basis. A challenge remains in performing end-to-end system security engineering for acquisition programs that are not scoped, or managed, to

include the entire system (e.g., block upgrades, segments). System security must be a holistic and continuous consideration in the design and development activity.

Systems of Systems in the Department of Defense

We begin with some definitions. A *system* is an integrated set of elements that accomplish a defined objective (INCOSE 2010, 5). A *capability* is the ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks (CJCS 2007, GL 6). A *system of systems* is a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities (US Department of Defense 2008, 4).

In the DoD, systems are employed in various combinations to provide war-fighter capabilities. In most cases the systems themselves were conceived, designed, engineered, developed, and deployed without explicit systems engineering of the larger SoS. With the growing importance of systems of systems to support capability needs, the DoD is increasingly recognizing the need to explicitly address priority capabilities. With this recognition, in selected cases, managers and systems engineers are given responsibility for the SoS, along with authority and resources. Examples include the Missile Defense Agency's Ballistic Missile Defense System, the Air Force's Air Operations Center, and the Navy's Integrated Fire Control—Counter Air initiative (DoD 2008). However, in these and most other cases, the individual systems in the SoS typically retain their own identities along with their own authorities, responsibilities, and resources to support their current and evolving user needs, with their own systems engineers and systems engineering processes. In a number of cases, systems are called upon to support multiple systems of systems as well as their original user needs. This makes the SoS an overlay on sets of new system developments and current systems, which themselves are evolving to meet changing demands.

For the purpose of this discussion, defense systems of systems can be seen as two types: the *platform SoS* in which military platforms (e.g., aircraft, ships, satellites) host various onboard systems (e.g., sensors, munitions) configured for particular applications; and the *mission-level SoS* (e.g., a set of systems working together to support a user operational mission). Both of these types of SoS challenge the application of systems engineering, since many of the models of systems engineering are based on the ability of the systems engineer to define boundaries and requirements clearly and to control the development environment so that requirements can be optimally allocated to components based on technical trade analyses.

Today's defense SoS environments make this approach impractical. Systems engineers are particularly challenged in mission-level systems of systems to

use existing systems as the components to meet user needs, so they are faced with suboptimal allocations of functionality and implementation details. In addition, without control over the development of the component systems that have independent ownership, funding, and development processes, the systems engineer needs to take into account considerations beyond the technical when evaluating capability-objective options. Finally, the environment changes during development, and unanticipated changes may have an overriding effect on user capabilities, further complicating the work of the systems engineer.

Implications of Systems of Systems for Security in Defense

As we discussed above, systems engineering and systems security engineering are applied to individual systems as part of the acquisition process. In most cases, systems engineering is not applied at the SoS level, and when it is, it does not often emphasize security for the SoS. The defense department's current guide for system-of-systems engineering is based on patterns of successful practice among systems engineers at the level of the SoS, and there is no discussion of security in the current version of the guide.

What are the implications of the lack of attention to systems security engineering for systems of systems? First, systems of systems are systems in their own right and logically should be a focus for protection planning and criticality analysis. By applying system security engineering only to individual systems in a mission-level SoS, vulnerabilities inherent in other systems in the "mission thread" could jeopardize the capability. For platform systems of systems, by addressing vulnerabilities of each of the systems (either the platform itself or the systems hosted on the platform) individually, vulnerabilities to the ensemble may persist. In both cases, the interfaces or connections between the systems introduce vulnerabilities. In short, ensuring the trustworthiness of individual systems does not guarantee that the SoS will be secure.

Second, applying security to systems in isolation may also lead to emphasis in the wrong places for effective security, potentially consuming needed resources in a time of scarcity. Unless one understands a system in its larger SoS context and mission, it is difficult to fully assess the vulnerability of that system. By assessing the security considerations across an SoS, it may be possible to determine which systems need different types of protection and more effectively apply limited security engineering resources. For example, complete perimeter-security defenses for individual systems within an SoS may be unnecessary if the SoS perimeter security is complete.

Since systems of systems are composed of systems developed under independent acquisition programs, analysis performed at any point in time will often encounter programs in different states of the lifecycle. The definition of the trade

space for system security engineering or any of the “ilities” will be key to ensuring key design attributes are built into each system and the SoS, as opposed to being bolted on when much of the design has been decided. The tendency is to postpone dealing with systems security engineering until “more is known.”

Finally, security is traditionally an activity that responds to a defined threat in a particular environment. With the emergent properties of systems of systems, the traditional sense of security does not apply and traditional perimeter security approaches are unlikely to succeed in a SoS with constantly changing boundaries and elements. Finally, since the SoS context is often dynamic, a system deemed “secure” in the context it was designed to support may exhibit new vulnerabilities when used in a changed or new context.

Systems Engineering Challenges and Opportunities


Addressing these implications is problematic for several reasons. In the Department of Defense today, as discussed above, limited attention is paid to understanding the broader SoS context for systems. Applying systems engineering to systems of systems is the exception rather than the rule, due in part to competing authorities and responsibilities across the SoS. The program manager of a given program operating within a SoS frequently does not have the responsibility or cognizance to address security of the entire SoS, just his or her piece and its integration.

Nonetheless, with the increased emphasis on capabilities and networking, the DoD is recognizing the criticality of effective end-to-end performance of systems of systems (SoS) to meet user needs, and the role of systems engineering is expanding to the engineering of SoS that provide user capabilities. This role needs to include consideration of security of systems of systems as well as of systems. What are the challenges and opportunities for security systems engineers as they recognize that systems of systems are systems in their own right and require protection planning and criticality analysis? What are the efficiencies of addressing security across systems? How do security systems engineers accommodate the heterogeneity and dynamics of systems of systems which challenge assumptions and approaches to security?

Addressing these provides both challenges and opportunities for the systems engineering community:

- **SoS Analysis:** How do we analyze an SoS to have the right set of data needed for a SoS-level criticality analysis? Are there analysis or architecture design approaches that could be applied to this problem?
- **SoS Security Metrics:** We do not have effective system or SoS-security metrics. Would the metrics for an SoS differ from those of a system? Would they differ between platform systems of systems and mission-level systems of systems?

- **SoS Architecture Approaches, Patterns, and Tools:** Are some approaches to structuring systems of systems demonstrated to be robust against different threats, and could these approaches be employed in the design to enhance security at the SoS level? For example, approaches may include data-continuity checking across systems; sharing of real-time risk assessment across systems, perhaps determined through distributed “honeypots”; or SoS configuration hopping so that adversaries cannot be confident of the configuration at any given point in time.
- **SoS Mission Assurance or SoS Link Dependencies:** We currently focus on the criticality of components to a system’s mission. If the SoS view looks at criticality of systems to an SoS mission, does anything change? If one SoS depends on another (e.g., an SoS depending on GPS for navigation), how do we assure the mission of each?
- **SoS System-Security Engineering:** If the SoS has a systems engineer, how can security be integrated into the systems engineering approach for the SoS? How can security be defined for a system whose boundaries and elements are constantly changing?

The first step in addressing these challenges is sharing relevant research and ongoing activity with the rest of the SoS and system-security engineering communities. The United States’ increasingly complex systems of systems and the threats that are facing them demand that we advance the discipline of systems security engineering to maintain confidence in our warfighting platforms and capabilities. 

Disclaimer

The opinions and statements in this article are those of the authors, not necessarily of the United States Department of Defense.

References

- Baldwin, K. 2009. “System Security Engineering: A Critical Discipline of Systems Engineering.” *INSIGHT* 12 (2): 11–13.
- Bayuk, J., et al. 2010. *System Security Engineering: A Research Roadmap*. Hoboken, NJ (US): Systems Engineering Research Center.
- CJCS (Chairman of the Joint Chiefs of Staff, United States). 2007. *Operation of the Joint Capabilities Integration and Development System*. CJCS Manual 3170.01C. Washington, DC: Joint Chiefs of Staff.
- Haskins, C. 2010. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Version 3.2. Revised by M. Krueger, D. Walden, and R. D. Hamelin. San Diego, CA (US): INCOSE.
- US Department of Defense. 2008. *Systems Engineering Guide for Systems of Systems*. Washington, DC.



INSIGHT

What's Inside

President's Corner

Special Feature

Systems of Systems and Self-Organizing Security	3
Systems of Systems and Security: A Defense Perspective	7
Securing a System of Systems: Start with the Threats that Put the Mission at Risk	7
A Model-Based Approach to Support Systems-of-Systems Security Engineering for Data Policies	11
Systems-of-Systems Issues in Security Engineering	15
Trading Security and Safety Risks within Systems of Systems	18
How Do We Measure Security?	22
Making People the Center of Systems Security	26
Security in the Age of Social Media: A Systems Engineering Challenge	30
Understanding Stigmergy as a Pattern in Self-Organizing Adversarial Systems of Systems	32
Architectural Patterns for Self-Organizing Systems-of-Systems	35

Fellows' Insight

Key Issues of Systems Engineering	42
How to Optimize a System	45

Forum

Toward a SoSEK, A Source of Systems Engineering Knowledge	45
---	----

Technical Operations

On the Right TRAK	46
-------------------	----

INCOSE Operations

Personal Reflections on the Value of Certification	50
--	----

SPECIAL FEATURE

Systems of Systems and Self-Organizing Security



(Photo: Amber Sports Used with permission)

INCOSE Events

System Engineering Events from Around the World	53
---	----

In Memoriam

In Memoriam A. Wayne Wymore	53
-----------------------------	----

Book Reviews

Ten Steps Ahead: What Separates Successful Business Visionaries from the Rest of Us	57
---	----

Final Thoughts

From the Chief Editor	62
-----------------------	----

INSIGHT

Publication of the International
Council on Systems Engineering

Chief Editor Bob Kenley
insight@incose.org
Assistant Editor +1 260 460 0054
andrew.cashner@incose.org Andrew Cashner
Theme Editors
rick.dove@incose.org Rick Dove
jennifer.bayuk@incose.org Jennifer Bayuk
Advertising Editor Christine Kowalski
advertising@incose.org +1 858 541 1725
Layout and Design Chuck Eng
chuck.eng@comcast.net +1 206 364 8696
Member Services INCOSE Administrative Office
info@incose.org +1 858 541-1725
On the Web <http://www.incose.org>
Article Submission INSIGHT@incose.org

Publication Schedule. *INSIGHT* is published four times per year. Issue and article/advertisement submission deadlines are as follows: **September 2011** Issue – 17 July; **December 2011** Issue – 15 October; **April 2012** Issue – 15 February; **July 2012** Issue – 15 May. For further information on submissions and issue themes, visit the INCOSE website as listed above.

Advertising in *INSIGHT*. Please see <http://www.incose.org/Products/Pubs/periodicals/insight.aspx> or e-mail advertising@incose.org.

Subscriptions to *INSIGHT* are available to INCOSE members as part of their membership. Complimentary copies are available on a limited basis. Back issues are available on the INCOSE website. To inquire about membership or to order a copy, contact Member Services.

©2011 Copyright Notice. Unless otherwise noted, the entire contents are copyrighted by INCOSE and may not be reproduced in whole or in part without written permission by INCOSE. Permission is given for use of up to three paragraphs as long as full credit is provided. The opinions expressed in *INSIGHT* are those of the authors and advertisers and do not necessarily reflect the positions of the editorial staff or the International Council on Systems Engineering.

Who are we? INCOSE is a 8000+ member organization of systems engineers and others interested in systems engineering. Its mission is to share, promote, and advance the best of systems engineering from across the globe for the benefit of humanity and the planet. INCOSE chapters worldwide, is sponsored by a corporate advisory board, and is led by elected officers, directors, and member board representatives.

2011 INCOSE Board of Directors

President: Samantha Robitaille, BAE Systems
President-Elect: John Thomas, Booz Allen Hamilton
Secretary: Richard Grzybowski, Corning, Inc.
Treasurer: Marsha Weiskopf, The Aerospace Corporation

Director for Academic Matters: Art Pyster, Stevens Institute of Technology
Director for Communications: Cecilia Haskins, Norwegian University of Science and Technology

Director for International Growth: Tat Soon Yeo, Temasek Defence Systems Institute

Director for Commercial Outreach: Henk van der Linden, SRON
Director for Strategy: Ralf Hartmann, Astrium Satellites

Corporate Advisory Board Chair: Andrew Pickard, Rolls Royce

Member Board Chair: Asmus Pandikow, Syntell AB, Sweden

Member Board Cochair: Eric Belle, Raytheon Corporation

Technical Director: Jean-Claude Roussel, EADS FRANCE IW

Director for Information Technology: Ryan Mortimer, Lockheed Martin

Managing Executive: Holly Witte, Universal Management Services, LLC

President's Corner

Systems for Summer

Samantha Robitaille, samantha.robitaille@incose.org



If you live in the Northern Hemisphere, it's likely that as you read this "President's Corner," you have already been planning for summer—unless, that is, your summer holiday has already started and you have selected *INSIGHT* as your preferred reading for a plane ride, or as you relax on a beach and keep an eye on the children. If you live in Australia, you might be reading this column at a lodge in the Snowy Mountains while the rest of your party is enjoying Tube Town.

As I write, memories of a particularly snowy winter in Michigan are almost forgotten, as we seem to have skipped spring and jumped straight into weather that feels like midsummer. However, having apparently missed spring altogether, I was fortunate enough to get a taste of autumn in early May with a trip to the SETE2011 conference in Canberra, Australia. It is certainly strange to see both spring flowers and autumn leaves in the space of 24 hours, but serves as a reminder of how small and yet diverse our world really is! More detail on the conference appears later in this issue.

I'm delighted to say that while I was there, members of the Systems Engineering Society of Australia (SESA) voted for the society to rejoin INCOSE. While there are some minor details still to be worked out, I am delighted that we are able to welcome the wider systems engineering community in Australia back into the INCOSE family and look forward to ongoing closer engagement. Australia will host the Asia-Pacific Conference on Systems Engineering (APCOSE) in 2012.

This latest agreement is one of a number that INCOSE leaders will sign this year. We have recently established agreements with both the Project Management Institute (PMI) and International Systems Safety Society (ISSS) to enable us to work more effectively with the professional organisations of other disciplines, so that systems engineers can do likewise. Such agreements reflect the connectivity of systems engineering across disciplines and domains, and across the globe. Establishing such agreements—and working to ensure that they mean more than just words on paper—has become a significant strategic effort for INCOSE and I am indebted to Ralf Hartmann, our director for strategy, who has been taking the lead on these efforts.

So what of planning for summer? INCOSE members in the United States may also be members of a certain "outdoors" store named REI, which seems to send almost daily e-mails to its members. In the past few weeks, it reminded us that we should be properly prepared if we head for the mountains this summer. It referenced Don Graydon's seminal text, *Mountaineering: The Freedom of the Hills* (Seattle, WA [US]: Mountaineers, 2010), which is now in its eighth edition and has sold over 600,000 copies since it was launched in the 1930s by The Mountaineers, a Seattle-based organization for climbers and outdoor adventurers.

What caught my eye was the reference to the 2003 edition, when the group's updated "systems" approach made its debut. Rather than the original list of essential items (a map, knife, compass, and other gear), the group recognised the functions that would, or might, be needed on an outdoor adventure and

» continues on next page